

#3

PATENT
81942.0010

Express Mail Label No. EL 713 696 005 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Yasuyuki MURAKAMI

Serial No: Not assigned

Filed: January 22, 2001

For: SECRET KEY REGISTRATION METHOD,
SECRET KEY REGISTER, SECRET KEY
ISSUING METHOD, CRYPTOGRAPHIC
COMMUNICATION METHOD AND
CRYPTOGRAPHIC COMMUNICATION
SYSTEM

Art Unit: Not assigned

Examiner: Not assigned



TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2000-016363 which was filed January 25, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON/L.L.P.

By: 

Louis A. Mok
Registration No. 22,585
Attorney for Applicant(s)

Date: January 22, 2001

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

#3

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

JCS62 U.S. PRO

09/767055



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 1月25日

出 願 番 号

Application Number:

特願2000-016363

出 願 人

Applicant(s):

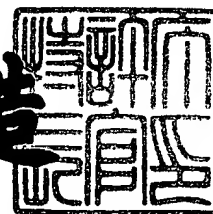
村田機械株式会社
笠原 正雄

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 8月18日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3064845

【書類名】 特許願

【整理番号】 20906

【提出日】 平成12年 1月25日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00
G09C 1/00

【発明の名称】 秘密鍵登録方法、秘密鍵登録器、秘密鍵発行方法、暗号
通信方法、暗号通信システム及び記録媒体

【請求項の数】 21

【発明者】

【住所又は居所】 京都府京都市伏見区竹田向代町 1 3 6 番地 村田機械株
式会社 本社工場内

【氏名】 村上 恭通

【特許出願人】

【識別番号】 000006297

【氏名又は名称】 村田機械株式会社

【代表者】 村田 純一

【特許出願人】

【識別番号】 597008636

【氏名又は名称】 笠原 正雄

【復代理人】

【識別番号】 100114557

【弁理士】

【氏名又は名称】 河野 英仁

【電話番号】 06-6944-4141

【代理人】

【識別番号】 100078868

【弁理士】

【氏名又は名称】 河野 登夫

【電話番号】 06-6944-4141

【手数料の表示】

【予納台帳番号】 001889

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9805283

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 秘密鍵登録方法、秘密鍵登録器、秘密鍵発行方法、暗号通信方法、暗号通信システム及び記録媒体

【特許請求の範囲】

【請求項 1】

暗号通信に利用する各エンティティ固有の秘密鍵の発行を複数の各センタへ要求する秘密鍵登録方法において、前記各エンティティは、基本パスワードと複数の異なる一方向性変換関数により複数のパスワードを生成し、前記各パスワードを前記各センタへ送付し、前記各センタから前記各パスワードで暗号化された各エンティティ固有の秘密鍵を受け取ることを特徴とする秘密鍵登録方法。

【請求項 2】

前記一方向性変換関数は一方向性ハッシュ関数であることを特徴とする請求項 1 に記載の秘密鍵登録方法。

【請求項 3】

前記エンティティは、前記各パスワードを公開鍵方式で暗号化して前記各センタへ送付することを特徴とする請求項 1 又は 2 に記載の秘密鍵登録方法。

【請求項 4】

暗号通信に利用する各エンティティ固有の秘密鍵の発行を複数の各センタへ要求する秘密鍵登録器において、基本パスワードと複数の異なる一方向性変換関数により複数のパスワードを生成する手段と、前記各パスワードを前記各センタへ送付する手段と、前記各センタから前記各パスワードで暗号化された各エンティティ固有の秘密鍵を受け取る手段と、を備えたことを特徴とする秘密鍵登録器。

【請求項 5】

前記一方向性変換関数は一方向性ハッシュ関数であることを特徴とする請求項 4 に記載の秘密鍵登録器。

【請求項 6】

前記送付手段は、前記各パスワードを公開鍵方式で暗号化して前記各センタへ送付することを特徴とする請求項 4 又は 5 に記載の秘密鍵登録器。

【請求項 7】

暗号通信に利用する各エンティティ固有の秘密鍵を複数の各センタにて発行する秘密鍵発行方法において、前記各エンティティは、基本パスワードと複数の異なる一方向性変換関数により複数のパスワードを生成し、前記各パスワードを前記各センタへ送り、前記各センタは、前記パスワードに基づいて暗号化された各エンティティ固有の秘密鍵を発行することを特徴とする秘密鍵発行方法。

【請求項 8】

前記一方向性変換関数は一方向性ハッシュ関数であることを特徴とする請求項 7 に記載の秘密鍵発行方法。

【請求項 9】

前記エンティティは、前記各パスワードを公開鍵方式で暗号化して前記各センタへ送付することを特徴とする請求項 7 又は 8 に記載の秘密鍵発行方法。

【請求項 10】

前記エンティティは、前記パスワード及び自身の電子メールアドレスをインターネットのホームページを介して送り、各センタは電子メールにて前記秘密鍵を発行することを特徴とする請求項 7 乃至 9 のいずれかに記載の秘密鍵発行方法。

【請求項 11】

前記エンティティは、前記パスワードを電子メールにより送り、前記各センタは電子メールにて前記秘密鍵を発行することを特徴とする請求項 7 乃至 9 のいずれかに記載の秘密鍵発行方法。

【請求項 12】

前記各センタは、各エンティティの特定情報を分割した分割特定情報を利用して各エンティティ固有の秘密鍵を発行することを特徴とする請求項 7 乃至 11 の何れかに記載の秘密鍵発行方法。

【請求項 13】

複数の各センタから各エンティティへ各エンティティ固有の特定情報を利用して作成した秘密鍵を送付し、一方のエンティティ側で、前記各センタから送付された該エンティティ固有の秘密鍵と送信相手である他方のエンティティの特定情報とから生成した共通鍵を用いて平文を暗号文にして他方のエンティティへ送信し、該他方のエンティティ側で、送信された暗号文を、前記各センタから送付さ

れた該エンティティ固有の秘密鍵と前記一方のエンティティの特定情報とから生成した、前記共通鍵と同一の共通鍵を用いて平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法において、前記各エンティティは、基本パスワードと複数の異なる一方向性変換関数により複数のパスワードを生成し、前記各パスワードを前記各センタへ送付し、前記各センタは、前記パスワードに基づいて暗号化された各エンティティ固有の秘密鍵を発行することを特徴とする暗号通信方法。

【請求項 1 4】

前記一方向性変換関数は一方向性ハッシュ関数であることを特徴とする請求項 1 3 に記載の暗号通信方法。

【請求項 1 5】

前記各エンティティは、秘密鍵方式で前記パスワードを前記各センタへ送付することを特徴とする請求項 1 3 又は 1 4 に記載の暗号通信方法。

【請求項 1 6】

複数の各センタから各エンティティへ各エンティティ固有の特定情報を利用して作成した秘密鍵を送付し、一方のエンティティ側で、前記各センタから送付された該エンティティ固有の秘密鍵と送信相手である他方のエンティティの特定情報とから生成した共通鍵を用いて平文を暗号文にして他方のエンティティへ送信し、該他方のエンティティ側で、送信された暗号文を、前記各センタから送付された該エンティティ固有の秘密鍵と前記一方のエンティティの特定情報とから生成した、前記共通鍵と同一の共通鍵を用いて平文に復号することにより、エンティティ間で情報の通信を行う暗号通信システムにおいて、基本パスワードと複数の異なる一方向性変換関数により複数のパスワードを生成し、前記各パスワードを前記各センタへ送付する複数のエンティティと、前記パスワードに基づいて暗号化された各エンティティ固有の秘密鍵を発行する複数のセンタと、を有することを特徴とする暗号通信システム。

【請求項 1 7】

前記一方向性変換関数は一方向性ハッシュ関数であることを特徴とする請求項 1 6 に記載の暗号通信システム。

【請求項 1 8】

前記複数のエンティティは、秘密鍵方式により前記パスワードを送付することを特徴とする請求項 1 6 又は 1 7 に記載の暗号通信システム。

【請求項 1 9】

コンピュータに、暗号通信に利用する各エンティティ固有の秘密鍵の発行を複数の各センタへ要求させるためのプログラムが記録されているコンピュータ読み取りが可能な記録媒体において、基本パスワードと複数の異なる一方向性変換関数により複数のパスワードを生成することをコンピュータに実行させる第 1 プログラムコード手段と、前記各パスワードを前記各センタへ送付することをコンピュータに実行させる第 2 プログラムコード手段と、前記各センタから前記各パスワードで暗号化された各エンティティ固有の秘密鍵を受け取ることをコンピュータに実行させる第 3 プログラムコード手段と、を含むことを特徴とするプログラムが記録されている記録媒体。

【請求項 2 0】

前記一方向性変換関数は、一方向性ハッシュ関数であることを特徴とする請求項 1 9 に記載の記録媒体。

【請求項 2 1】

前記第 2 プログラムコード手段は、公開鍵方式により前記パスワードを前記各センタへ送付すること特徴とする請求項 1 9 又は 2 0 に記載の記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、エンティティ間の暗号通信に利用される各エンティティ固有の秘密鍵を発行する秘密鍵発行方法、秘密鍵発行器、エンティティ間にて暗号通信を行う暗号通信方法、暗号通信システム、及びそれらに用いられるプログラムを記録した記録媒体に関する。

【0 0 0 2】

【従来技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤と

して、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュタリソースの共有」、「マルチアクセス」、「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事、外交面で用いられてきた暗号技術が注目されている。

【 0 0 0 3 】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【 0 0 0 4 】

暗号化鍵と復号鍵とは、等しくても良いし、異なっても良い。両者の鍵が等しい暗号方式は、共通鍵暗号方式と呼ばれ、米国商務省標準局が採用した DES (Data Encryption Standard) はその典型例である。このような共通鍵暗号方式の従来例は、次のような 3 種の方法に分類できる。

【 0 0 0 5 】

① 第 1 の方法

暗号通信を行う可能性がある相手との共通鍵をすべて秘密保管しておく方法

② 第 2 の方法

暗号通信の都度、呼び通信により鍵を共有し合う方法（Diffie-Hellman による鍵共有方式、公開鍵方式による鍵配送方式等）。

③ 第 3 の方法

各ユーザ（エンティティ）の氏名、住所等の個人を特定する公開された特定情報（ID（Identity）情報）を利用して、予備通信を行うことなく、送信側のエンティティ、受信側のエンティティが独立に同一の共通鍵を生成する方法（KPS（Key Predistribution System）、ID-NIKS（ID-based Non-Interactive Key Sharing Schemes）等）。

【0006】

第1の方法では、通信相手の共通鍵を保管しておく必要がある。また、第2の方法は、鍵共有のための予備通信が必要である。第3の方法は、通信相手の共通鍵を保管する必要もなく、予備通信も不要であり、公開された相手のID情報とセンタから予め配布されている固有の秘密パラメータとを用いて、必要時に、任意の相手との共通鍵を生成できるので、便利な方法である。

【0007】

図11は、このID-NIKSのシステムの原理を示す図である。信頼できるセンタの存在を仮定し、このセンタを中心にして共通鍵生成システムを構成している。図11において、エンティティXの特定情報であるエンティティXの名前、住所、電話番号等のID情報は、ハッシュ関数 $h(\cdot)$ を用いて $h(ID_X)$ で表す。センタは任意のエンティティXに対して、センタ公開情報 $\{PC_i\}$ 、センタ秘密情報 $\{SC_i\}$ 及びエンティティXのID情報 $h(ID_X)$ に基づいて、以下のように秘密鍵 S_{Xi} を計算し、秘密裏にエンティティXへ配布する。

$$S_{Xi} = F_i(\{SC_i\}, \{PC_i\}, h(ID_X))$$

【0008】

エンティティXは他の任意のエンティティYとの間で、暗号化、復号のための共通鍵 K_{XY} を、エンティティX自身の秘密鍵 $\{S_{Xi}\}$ 、センタ公開情報 $\{PC_i\}$ 及び相手先のエンティティYのID情報 $h(ID_Y)$ を用いて以下のように生成する。

$$K_{XY} = f(\{S_{Xi}\}, \{PC_i\}, h(ID_Y))$$

また、エンティティYも同様にエンティティXへの共通鍵 K_{YX} を生成する。もし常に $K_{XY} = K_{YX}$ の関係が成立すれば、この鍵 K_{XY} 、 K_{YX} をエンティティX、Y間

で暗号化鍵、復号鍵として使用できる。

【 0 0 0 9 】

本発明者等は、このような I D - N I K S について種々の暗号化方法、共通鍵生成方法、暗号通信方法等を提案しており、また、各エンティティの I D 情報を複数に分割して複数の各センタからその分割 I D 情報に基づく秘密鍵をエンティティに配布する構成にして、より安全性を高めるようにした I D - N I K S による暗号化方法、共通鍵生成方法、暗号通信方法等についても、提案している。

【 0 0 1 0 】

上記提案においては、自身固有の秘密鍵の発行を希望する各エンティティは、例えば、各センタのホームページにアクセスしてサーバを介して、または、電子メールにて直接的に、自身のパスワードを公開鍵方式で各センタへ送付する。各センタは、この送られた各エンティティのパスワードに基づいて自身の秘密情報を暗号化して、つまりそのパスワードを自身の秘密情報に盛り込んだ秘密鍵方式で、各エンティティ固有の秘密鍵を、例えば電子メールにて各エンティティへ発行する。よって、各エンティティの秘密鍵が自身のパスワードを盛り込んで暗号化されて発行されるので、その秘密鍵が他者に知られることがなく安全に秘密鍵を発行できる。

【 0 0 1 1 】

【発明が解決しようとする課題】

各エンティティが複数の各センタへパスワードを送付するが、安全のためには、各エンティティは、各センタ毎に固有のパスワードを送付することが望ましい。しかしながら、各エンティティにおいて、センタ数に応じたパスワードを管理する必要が生じていた。

【 0 0 1 2 】

本発明は斯かる事情に鑑みてなされたものであり、各エンティティにおいて、管理するパスワードの数を少なくすることが可能な秘密鍵登録方法、秘密鍵発行方法、暗号通信方法等を提供することを目的とする。

【 0 0 1 3 】

【課題を解決するための手段】

本発明の秘密鍵登録方法は、暗号通信に利用する各エンティティ固有の秘密鍵の発行を複数の各センタへ要求する秘密鍵登録方法において、前記各エンティティは、基本パスワードと複数の異なる一方向性変換関数により複数のパスワードを生成し、前記各パスワードを前記各センタへ送付し、前記各センタから前記各パスワードで暗号化された各エンティティ固有の秘密鍵を受け取ることを特徴とする。

【 0 0 1 4 】

また、本発明の秘密鍵登録器は、暗号通信に利用する各エンティティ固有の秘密鍵の発行を複数の各センタへ要求する秘密鍵登録器において、基本パスワードと複数の異なる一方向性変換関数により複数のパスワードを生成する手段と、前記各パスワードを前記各センタへ送付する手段と、前記各センタから前記各パスワードで暗号化された各エンティティ固有の秘密鍵を受け取る手段と、を備えたことを特徴とする。

【 0 0 1 5 】

また、本発明の秘密鍵発行方法においては、暗号通信に利用する各エンティティ固有の秘密鍵を複数の各センタにて発行する秘密鍵発行方法において、前記各エンティティは、基本パスワードと複数の異なる一方向性変換関数により複数のパスワードを生成し、前記各パスワードを前記各センタへ送り、前記各センタは、前記パスワードに基づいて暗号化された各エンティティ固有の秘密鍵を発行することを特徴とする。

【 0 0 1 6 】

また、本発明の暗号通信方法においては、複数の各センタから各エンティティへ各エンティティ固有の特定情報を利用して作成した秘密鍵を送付し、一方のエンティティ側で、前記各センタから送付された該エンティティ固有の秘密鍵と送信相手である他方のエンティティの特定情報とから生成した共通鍵を用いて平文を暗号文にして他方のエンティティへ送信し、該他方のエンティティ側で、送信された暗号文を、前記各センタから送付された該エンティティ固有の秘密鍵と前記一方のエンティティの特定情報とから生成した、前記共通鍵と同一の共通鍵を用いて平文に復号することにより、エンティティ間で情報の通信を行う暗号通信

方法において、前記各エンティティは、基本パスワードと複数の異なる一方向性変換関数により複数のパスワードを生成し、前記各パスワードを前記各センタへ送付し、前記各センタは、前記パスワードに基づいて暗号化された各エンティティ固有の秘密鍵を発行することを特徴とする。

【0017】

また、本発明の暗号通信システムにおいては、複数の各センタから各エンティティへ各エンティティ固有の特定情報を利用して作成した秘密鍵を送付し、一方のエンティティ側で、前記各センタから送付された該エンティティ固有の秘密鍵と送信相手である他方のエンティティの特定情報とから生成した共通鍵を用いて平文を暗号文にして他方のエンティティへ送信し、該他方のエンティティ側で、送信された暗号文を、前記各センタから送付された該エンティティ固有の秘密鍵と前記一方のエンティティの特定情報とから生成した、前記共通鍵と同一の共通鍵を用いて平文に復号することにより、エンティティ間で情報の通信を行う暗号通信システムにおいて、基本パスワードと複数の異なる一方向性変換関数により複数のパスワードを生成し、前記各パスワードを前記各センタへ送付する複数のエンティティと、前記パスワードに基づいて暗号化された各エンティティ固有の秘密鍵を発行する複数のセンタと、を有することを特徴とする。

【0018】

また、本発明のコンピュータ読み取りが可能な記録媒体は、コンピュータに、暗号通信に利用する各エンティティ固有の秘密鍵の発行を複数の各センタへ要求させるためのプログラムが記録されているコンピュータ読み取りが可能な記録媒体において、基本パスワードと複数の異なる一方向性変換関数により複数のパスワードを生成することをコンピュータに実行させる第1プログラムコード手段と、前記各パスワードを前記各センタへ送付することをコンピュータに実行させる第2プログラムコード手段と、前記各センタから前記各パスワードで暗号化された各エンティティ固有の秘密鍵を受け取ることをコンピュータに実行させる第3プログラムコード手段と、を含むことを特徴とする。

【0019】

また、上記発明において、前記一方向性変換関数は一方向性ハッシュ関数であ

ることを特徴とする。

【 0 0 2 0 】

また、上記発明において、前記エンティティは、前記各パスワードを公開鍵方式で暗号化して前記各センタへ送付することを特徴とする。

【 0 0 2 1 】

また、上記発明において、前記エンティティは、前記パスワード及び自身の電子メールアドレスをインターネットのホームページを介して送り、各センタは電子メールにて前記秘密鍵を発行することを特徴とする。

【 0 0 2 2 】

また、上記発明において、前記エンティティは、前記パスワードを電子メールにより送り、前記各センタは電子メールにて前記秘密鍵を発行することを特徴とする。

【 0 0 2 3 】

また、上記発明において、前記各センタは、各エンティティの特定情報を分割した分割特定情報を利用して各エンティティ固有の秘密鍵を発行することを特徴とする。

【 0 0 2 4 】

本発明では、自身固有の秘密鍵の発行を希望するエンティティは、基本パスワードと一方向性変換関数に基づいて、センタ数に応じた複数のパスワードを生成し、生成されたパスワードを各センタへ送付するの、各エンティティにおいて管理する必要があるパスワードの数を少なくすることができる。

【 0 0 2 5 】

また、本発明では、一方向性変換関数として一方向性ハッシュ関数を利用することができる。さらに、各エンティティがパスワードを公開鍵方式で暗号化して各センタへ送付するので、パスワードを安全に送付することができる。

【 0 0 2 6 】

また、本発明では、エンティティからインターネットのホームページを使用して、パスワード及び自身の電子メールアドレスを送付することにより、電子メールアドレスも暗号化して、センタへ送付することができ、より安全性が向上する

【 0 0 2 7 】

また、本発明では、エンティティから電子メールを使用して、パスワードを送付することにより、エンティティでは、自身の電子メールアドレスをあらためて入力する必要がない。

【 0 0 2 8 】

また、本発明では、各エンティティの特定情報（ID情報）の分割情報を利用して、各エンティティ固有の秘密鍵を発行することにより、安全性が高いID-NIKSによるエンティティ間の暗号通信を行うことができる。

【 0 0 2 9 】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図1は、本発明の暗号通信システムの構成を示す模式図である。情報の隠匿を信頼できる複数（K個）のセンタ1が、秘密鍵発行のサーバとして設定されている。なお、これらのセンタ1としては、例えば社会の公的機関を想定できる。

【 0 0 3 0 】

これらの各センタ1と、この暗号通信システムを利用するユーザとしての複数の各エンティティa, b, ..., zとは、通信路 2_{a1} , ..., 2_{aK} , 2_{b1} , ..., 2_{bK} , ..., 2_{z1} , ..., 2_{zK} により接続されており、これらの通信路を介して、各エンティティa, b, ..., zから各センタ1へ秘密鍵発行の依頼がなされ、各センタ1から各エンティティ固有の秘密鍵が各エンティティa, b, ..., zへ発行されるようになっている。また、2人のエンティティ間には電子メールによる通信路 3_{ab} , 3_{az} , 3_{bz} , ...が設けられており、通信情報を暗号化した暗号文が互いのエンティティ間で電子メールにより送受信されるようになっている。

【 0 0 3 1 】

図2は、2人のエンティティa, b間における情報の通信状態を示す模式図である。図2の例は、エンティティaが平文（メッセージ）Mを暗号文Cに暗号化してそれをエンティティbへ送信し、エンティティbがその暗号文Cを元の平文（メッセージ）Mに復号する場合を示している。

【0032】

総数K個の各センタ1には、自身の秘密情報（対称行列）から各エンティティ a, b 毎に選択したものを各エンティティのパスワードに基づいて暗号化して各エンティティ a, b 固有の秘密鍵を発行する秘密鍵発行器2が備えられている。秘密鍵発行器2は、その内部構成を示す図3に表すように、暗号化された秘密情報を格納する秘密情報格納部3と、秘密情報格納部3に格納されている暗号化秘密情報を読み出して復号する秘密情報復号部4と、センタ1自身の秘密情報と各エンティティ a, b の特定情報（ID情報）から各エンティティ a, b 固有の秘密鍵を作成する秘密鍵作成部5と、作成された秘密鍵を各エンティティ a, b から入力されたパスワードで暗号化する秘密鍵暗号化部6と、所定周期毎に更新されるセンタ1の秘密情報を暗号化して秘密情報格納部3に書き込む秘密情報更新部6とを有する。

【0033】

エンティティ a 側には、K個の各センタ1に対して秘密鍵の発行を要求する登録部10と、K個の各センタ1から送られる秘密鍵方式でのエンティティ a 自身固有の秘密鍵を復号する第1秘密鍵復号部11と、復号されたK個の自身固有の秘密鍵を暗号化する秘密鍵暗号化部12と、暗号化された秘密鍵を格納する秘密鍵格納部13と、秘密鍵格納部13に格納されている暗号化秘密鍵を読み出して復号する第2秘密鍵復号部14と、自身固有の秘密鍵とエンティティ b の特定情報（ID情報）とに基づいてエンティティ a が求めるエンティティ b との共通鍵 K_{ab} を生成する共通鍵生成部15と、共通鍵 K_{ab} を用いて平文（メッセージ）M を暗号文Cに暗号化して電子メールによる通信路30へ出力する平文暗号化部16と、共通鍵、平文、暗号文等を表示する表示部17とが備えられている。

【0034】

また、エンティティ b 側には、K個の各センタ1に対して秘密鍵の発行を要求する登録部20と、K個の各センタ1から送られる秘密鍵方式でのエンティティ b 自身固有の秘密鍵を復号する第1秘密鍵復号部21と、復号されたK個の自身固有の秘密鍵を暗号化する秘密鍵暗号化部22と、暗号化された秘密鍵を格納する秘密鍵格納部23と、秘密鍵格納部23に格納されている暗号化秘密鍵を読み

出して復号する第2秘密鍵復号部24と、自身固有の秘密鍵とエンティティaの特定情報(ID情報)とに基づいてエンティティbが求めるエンティティaとの共通鍵 K_{ba} を生成する共通鍵生成部25と、共通鍵 K_{ba} を用いて通信路30から入力した暗号文Cを平文(メッセージ)Mに復号して出力する暗号文復号部26と、共通鍵、平文、暗号文等を表示する表示部27とが備えられている。

【0035】

次に、このような構成の暗号通信システムにおける暗号通信の処理動作について説明する。

【0036】

(予備処理)

各エンティティを特定する特定情報(ID情報)、例えばそのエンティティの電子メールアドレスを表すIDベクトル(Lビット2進ベクトル)を、図4に示すように、ブロックサイズMビット毎にK個のブロックに分割する。例えば、エンティティaの電子メールアドレスを示すIDベクトル(ベクトル I_a)を式(1)のように分割する。分割特定情報である各ベクトル I_{aj} ($j=1, 2, \dots, K$)を分割IDベクトルと呼ぶ。なお、エンティティの電子メールアドレスが、ハッシュ関数によってLビットのIDベクトルに変換される。

【0037】

【数1】

$$\overrightarrow{I_a} = [\overrightarrow{I_{a1}} | \overrightarrow{I_{a2}} | \dots | \overrightarrow{I_{aK}}] \quad \dots (1)$$

【0038】

(秘密鍵発行処理(エンティティの登録処理))

図5及び図6に、エンティティa, bの登録部10、20によるセンタへの登録処理及び、各センタ1の秘密鍵発行器2による秘密鍵発行処理を示す。この暗号通信システムに参加したいエンティティa, b、即ち、自身固有の秘密鍵の発行を希望するエンティティa, bは、各センタ1(センタ第1、第2、…、第K)へ登録し、秘密鍵を入手する。

【0039】

まず、図5（I）に示すように、エンティティ a では、基本パスワードと自身の電子メールアドレスを登録部10へ入力する（S111）。登録部10は、基本パスワードと一方向性変換関数に基づいて、センタ第1用のパスワードを生成し（S112）、センタ第1への登録処理を行い、センタ第1から秘密鍵を入手する（S113）。

【0040】

同様に、それぞれ異なる一方向性変換関数を用いて、センタ第2用、センタ第K用のパスワードを生成し、センタ第2、センタ第Kへの登録処理を行い、秘密鍵を入手する（S114～S117）。同様に、図5（II）に示すように、エンティティ b においても、登録部20により各センタ1への登録処理を行い、各センタ1から秘密鍵を入手する（S121～127）。

【0041】

次に、図6を参照しながら、エンティティ a におけるセンタ第1への登録処理及びセンタ第1におけるエンティティ a の秘密鍵発行処理について説明する。他のエンティティにおける登録処理及び他のセンタにおける秘密鍵発行処理についても同様である。

【0042】

エンティティ a の登録部10では、S112で生成されたセンタ第1用のパスワードを取り込み（S211）、センタ第1のホームページにアクセスしてサーバを介して、パスワードとエンティティ a 自身の電子メールアドレスとを公開鍵方式（SSL等）で暗号化しセンタ第1へ送信する（S212，S213）。

【0043】

センタ第1の秘密鍵発行器2では、秘密情報格納部3に格納されている暗号化秘密情報を秘密情報復号部4で復号した秘密情報（後述する対称行列）を得る（S221）。また、エンティティ a から公開鍵方式で暗号化されたパスワードと電子メールアドレスを受信し（S222）、復号する（S223）。秘密鍵作成部5にて、エンティティ a の電子メールアドレスから得られた分割IDベクトルに対応する部分を選択し、エンティティ a の秘密鍵（後述する秘密鍵ベクトル）を生成する（S224）。

【 0 0 4 4 】

生成した秘密鍵（秘密鍵ベクトル）をエンティティ a から受信したパスワードに基づいて暗号化して（S 2 2 5）、即ち、選択した秘密鍵（秘密鍵ベクトル）にパスワードを盛り込んだ秘密鍵方式で、そのエンティティ固有の秘密鍵を、電子メールを介してそのエンティティに発行する（S 2 2 6）。この際の秘密鍵方式としては、DESを利用できる。なお、エンティティの電子メールアドレスを暗号化して送付するようにしても良い。

【 0 0 4 5 】

エンティティ a は、暗号化されたエンティティ a の秘密鍵（秘密鍵ベクトル）を受信し（S 2 1 4）、パスワードを用い、第 1 秘密鍵復号部 1 1 で復号する（S 2 1 5）。さらに、復号した秘密鍵（秘密ベクトル）は安全のため、一旦、秘密鍵暗号化部 1 2 で暗号化されて（S 2 1 6）、秘密鍵格納部 1 3 に格納される。

【 0 0 4 6 】

同様にしてエンティティ a は、センタ第 2、・・・、第 K へ登録を行い、秘密鍵を入手する。上述のように、各センタ 1 によって発行された各エンティティの秘密鍵（秘密鍵ベクトル）は、パスワードによって各センタ 1 で暗号化されてから各エンティティへ送付され、各エンティティで復号されるので、各エンティティは秘密鍵（秘密鍵ベクトル）を秘密裡に入手することができる。

【 0 0 4 7 】

安全のためには、各センタ 1 毎にそれぞれ固有のパスワードを送付することが望ましいが、パスワードの管理が煩雑になる可能性がある。そこで、1 つの基本パスワードと一方向性変換関数に基づいて、複数のパスワードを生成することにより、管理が必要なパスワード数を削減することができる。また、一方向性変換関数を秘密にすることにより、安全性が損なわれることはない。

【 0 0 4 8 】

1 つの基本パスワードと一方向性変換関数に基づいて複数のパスワードを生成するには、次のような方法がある。

①各センタ 1 毎に異なる一方向性変換関数を使用する。

②基本パスワードに各センタ毎に異なるスクランブル処理を施したり、各センタ毎に連番を付加するなどしてから、各センタ1で共通又は各センタ1毎に異なる一方向性変換関数を使用する。

【0049】

また、一方向性変換関数として一方向性ハッシュ関数を用いることができる。一方向性ハッシュ関数による演算後のパスワードは、元の基本パスワードよりデータ長が短くなるので、不都合であれば、適宜、異なる複数の一方向性ハッシュ関数による演算結果を組み合わせてパスワードを構成する。このようにすれば、一方向性ハッシュ関数による、データ長の低減を補うことができる。

【0050】

なお、より簡易的に、電子メールにより、エンティティの登録処理及び秘密鍵の発行処理を行うことも可能である。この場合、自身固有の秘密鍵の発行を希望するエンティティは、自身のパスワードを電子メールにて直接各センタ1へ公開鍵方式で送る。各センタ1では、上記の場合と同様に、秘密情報からエンティティに対応して選択した秘密鍵にエンティティ側で入力されたパスワードを盛り込んだ秘密鍵方式（DES等）でそのエンティティ固有の秘密鍵を、電子メールを介してそのエンティティに発行する。

【0051】

なお、上述した例では、電子メールにて秘密鍵を発行するようにしているが、ICカード等の可搬型の記録媒体にエンティティ固有の秘密鍵を書き込み、その記録媒体をエンティティへ送るようにすることも可能である。

【0052】

ここで、各センタ1での秘密情報（対称行列）、及び、各エンティティ固有の秘密鍵（秘密鍵ベクトル）の具体的内容について説明する。 j （ $j = 1, 2, \dots, K$ ）番目のセンタ1は、秘密情報として、ランダムな数を要素とする対称行列 H_j （ $2^M \times 2^M$ ）を有している。そして、エンティティ a に対して、対称行列 H_j のそのエンティティの分割IDベクトルに対応する行ベクトルを秘密鍵（秘密鍵ベクトル）として発行する。即ち、エンティティ a に対しては、 H_j 〔ベクトル I_{aj} 〕を発行する。この H_j 〔ベクトル I_{aj} 〕は、対称行列 H_j よりベクトル

ル I_{aj} に対応した行を 1 行抜き出したベクトルを表す。

【0053】

ここで、エンティティ側でのパスワード入力の例について説明する。パスワード入力処理については、パスワード入力が不慣れなエンティティにとって特に、次のような 2 つの例が好適である。

【0054】

一方の例では、各エンティティが文字列を入力し、その入力データを base 64 でエンコードしたものをパスワードとする。この場合、64 種の各 1 つの文字入力にて 6 ビットのデータを表せるので、パスワードが 64 ビットである場合には、11 個の文字を入力すれば良いことになる。

【0055】

また、他方の例では、0～9 及び A～F の 16 種の文字を入力することを原則として、これらの 16 種の文字以外が入力された場合には、その文字を 0～9, A～F の何れかの文字に置換する。

【0056】

(エンティティ a, b における共通鍵の生成処理)

エンティティ a, b における共通鍵生成処理について、図 7 を参照しながら説明する。エンティティ a (エンティティ b) は、通信相手であるエンティティ b (エンティティ a) との共通鍵 K_{ab} (K_{ba}) を生成する際に、暗号化された秘密鍵 (秘密鍵ベクトル) を秘密鍵格納部 13 (23) から読み出して、第 2 秘密鍵復号部 14 (24) で再び秘密鍵 (秘密鍵ベクトル) を復号する (S311 (S321))。

【0057】

エンティティ a (エンティティ b) は、共通鍵を生成するために相手のエンティティ b (エンティティ a) の特定情報 (ID 情報) としての電子メールアドレスを必要とする。送信側となるエンティティ a においては、エンティティ b の電子メールアドレスは送信相手先の電子メールアドレスとして与えられる。また、受信側となるエンティティ b においては、エンティティ a の電子メールアドレスは受信した電子メールの発信元情報 (From フィールド等) から得ることがで

きる (S322)。

【0058】

共通鍵生成部15(25)にて、各センタ1から受け取った秘密鍵(秘密鍵ベクトル)のうち、エンティティb(エンティティa)の特定情報(ID情報)に基づいて、対応する要素を取り出し、これらK個の要素を合成して、エンティティa(エンティティb)のエンティティb(エンティティa)に対する共通鍵 K_{ab} (K_{ba})を生成する(S312(S323))。ここで、K個の各センタが有する秘密情報(行列)の対称性に基づいて、両共通鍵 K_{ab} , K_{ba} は一致する。

【0059】

エンティティa, bの特定情報(ID情報)として、電子メールアドレスを利用している。図8に示すように、電子メールアドレスはメールシステムによって、ドメイン名が付いているもの(図8(I))と、付いていないもの(図8(II))がある。ドメイン名が付いている電子メールアドレスはインターネットの電子メールアドレスとして使用されている。また、インターネット以外のメールシステムにおいては、ドメイン名が付いていない電子メールアドレスを使用していることもある。

【0060】

ゲートウェイを介してインターネットに接続されたLAN環境においては、これら2種類の電子メールアドレスのいずれでも使用できる場合がある。例えば、LANなどの閉じた範囲では、いずれの電子メールアドレスでも使用可能であり、ゲートウェイを介してインターネットメールを使用する場合には、ドメイン名が付いている電子メールアドレスを使用するようになっている。

【0061】

エンティティa, bにおいては、インターネットの電子メールにより、各センタから秘密鍵(秘密鍵ベクトル)を入手した場合には、ドメイン名が付いている電子メールアドレスに基づいて秘密鍵(秘密鍵ベクトル)が生成されている。したがって、共有鍵を生成する相手の電子メールアドレスにドメイン名が付いていなければ、共通鍵を正しく生成できなくなり、暗号通信を行うことができない。

【0062】

そこで、図 9 (I) 及び図 9 (II) に示すように、送信側となるエンティティ a において、相手先として指定されたエンティティ b の電子メールアドレスにドメイン名が付いていない場合には (S 4 1 1)、エンティティ a と同じドメイン名を付けて (S 4 1 2)、共通鍵 K_{ab} の生成を行うようにした (S 4 1 3)。

【0063】

また、受信側となるエンティティ b において、エンティティ a から受信した電子メールの発信元情報 (From フィールド) 等の電子メールアドレスに、ドメイン名が付いていない場合には (S 4 2 1)、エンティティ b と同じドメイン名を付けて (S 4 2 2)、共通鍵 K_{ba} の生成を行うようにした (S 4 2 3)。

【0064】

(エンティティ a における暗号化処理、エンティティ b における復号処理)

図 7 に戻り、エンティティ a にあって、共通鍵生成部 1 5 で生成された共通鍵 K_{ab} を用いて、平文暗号化部 1 6 にて、平文 (メッセージ) M が暗号文 C に暗号化されて (S 3 1 3)、その暗号文 C が電子メールによる通信路 3 0 へ送信される (S 3 1 4)。エンティティ b にあって、共通鍵生成部 2 5 で生成された共通鍵 K_{ba} を用いて、暗号文復号部 2 6 にて、暗号文 C が元の平文 (メッセージ) M に復号される (S 3 2 4)。

【0065】

図 1 0 は、本発明の記録媒体の実施例の構成を示す図である。ここに例示するプログラムは、秘密鍵の発行を各センタへ依頼する登録処理、各エンティティからの依頼に基づいて各センタにおいて各エンティティ固有の秘密鍵を発行する上述したような秘密鍵発行処理、各センタから秘密鍵方式で発行された秘密鍵を各エンティティにおいて復号する上述したような秘密鍵復号処理、自身固有の秘密鍵を用いて通信相手との間の共通鍵を生成する上述したような共通鍵作成処理、センタの秘密情報 (対称行列)、各エンティティの秘密鍵 (秘密鍵ベクトル) を暗号化して格納する上述したような秘密情報、秘密鍵の格納・更新処理、共通鍵、平文、暗号文を表示する上述したような表示処理、及び／または、平文の暗号化処理、暗号文の復号処理等を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ 4 0 は、各ホスト側または各エンティティ側に設け

られている。

【0066】

図10において、コンピュータ40とオンライン接続する記録媒体41は、コンピュータ40の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体41には前述の如きプログラム41aが記録されている。記録媒体41から読み出されたプログラム41aがコンピュータ40を制御することにより、少なくとも1つの上記処理を実行する。

【0067】

コンピュータ40の内部に設けられた記録媒体42は、内蔵設置される例えばハードディスクドライブまたはROM等を用いてなり、記録媒体42には前述の如きプログラム42aが記録されている。記録媒体42から読み出されたプログラム42aがコンピュータ40を制御することにより、少なくとも1つの上記処理を実行する。

【0068】

コンピュータ40に設けられたディスクドライブ40aに装填して使用される記録媒体43は、運搬可能な例えば光磁気ディスク、CD-ROMまたはフレキシブルディスク等を用いてなり、記録媒体43には前述の如きプログラム43aが記録されている。記録媒体43から読み出されたプログラム43aがコンピュータ40を制御することにより、少なくとも1つ以上の上記処理を実行する。

【0069】

【発明の効果】

以上詳述したように、本発明では、自身固有の秘密鍵の発行を希望するエンティティは、基本パスワードと一方向性変換関数に基づいてセンタ数に応じた複数のパスワードを生成するので、各エンティティにおいて管理する必要があるパスワードの数を少なくすることができる。

【図面の簡単な説明】

【図1】

本発明の暗号通信システムの構成を示す模式図である。

【図2】

2 個のエンティティ間における情報の通信状態を示す模式図である。

【図 3】

秘密鍵発行器の内部構成を示す図である。

【図 4】

エンティティの ID ベクトル（特定情報）分割例を示す模式図である。

【図 5】

エンティティにおける登録処理を示す流れ図である。

【図 6】

エンティティにおける登録処理及びセンタにおける秘密鍵発行処理を示す流れ図である。

【図 7】

エンティティ間における共通鍵生成及処理、暗号化処理及び復号処理を示す流れ図である。

【図 8】

電子メールアドレスの例を示す図である。

【図 9】

共通鍵生成処理を示す流れ図である。

【図 1 0】

記録媒体の実施例の構成を示す図である。

【図 1 1】

ID-NIKS のシステムの原理構成図である。

【符号の説明】

- 1 センタ
- 2 秘密鍵発行器
- 5 秘密鍵生成部
- 1 0, 2 0 秘密鍵登録部
- 1 5, 2 5 共通鍵生成部
- 1 6 平文暗号化部
- 2 6 暗号文復号部

3 0 通信路

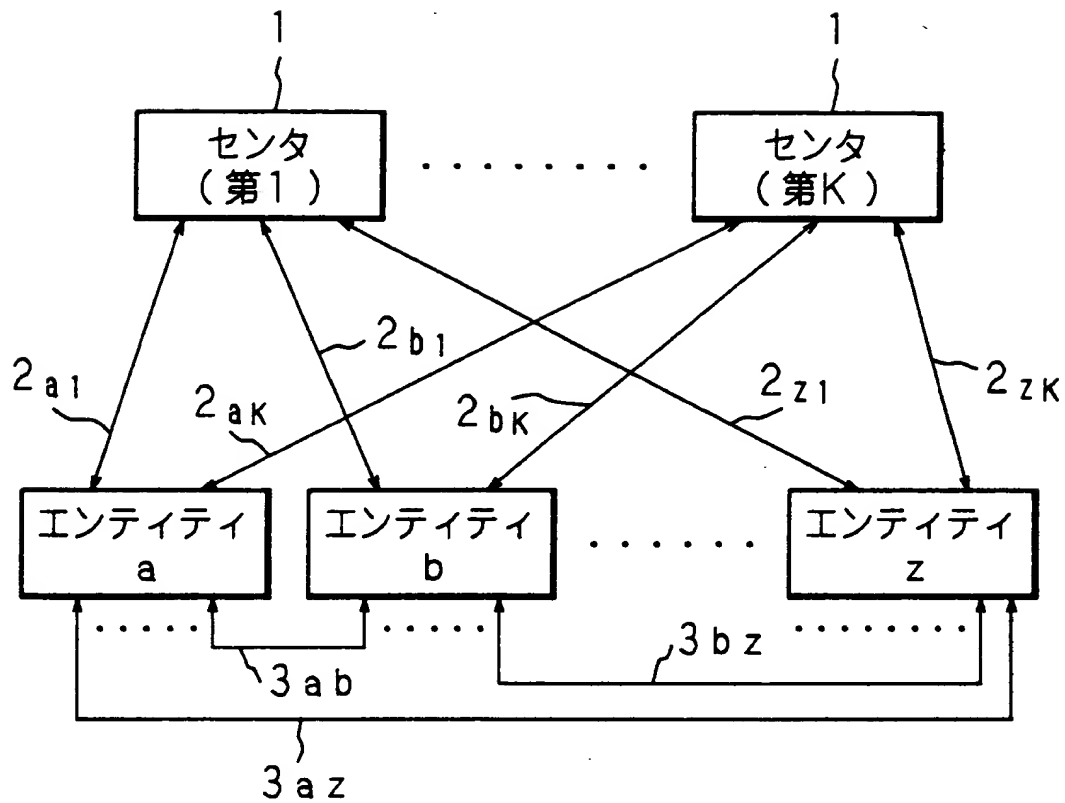
4 0 コンピュータ

4 1, 4 2, 4 3 記録媒体

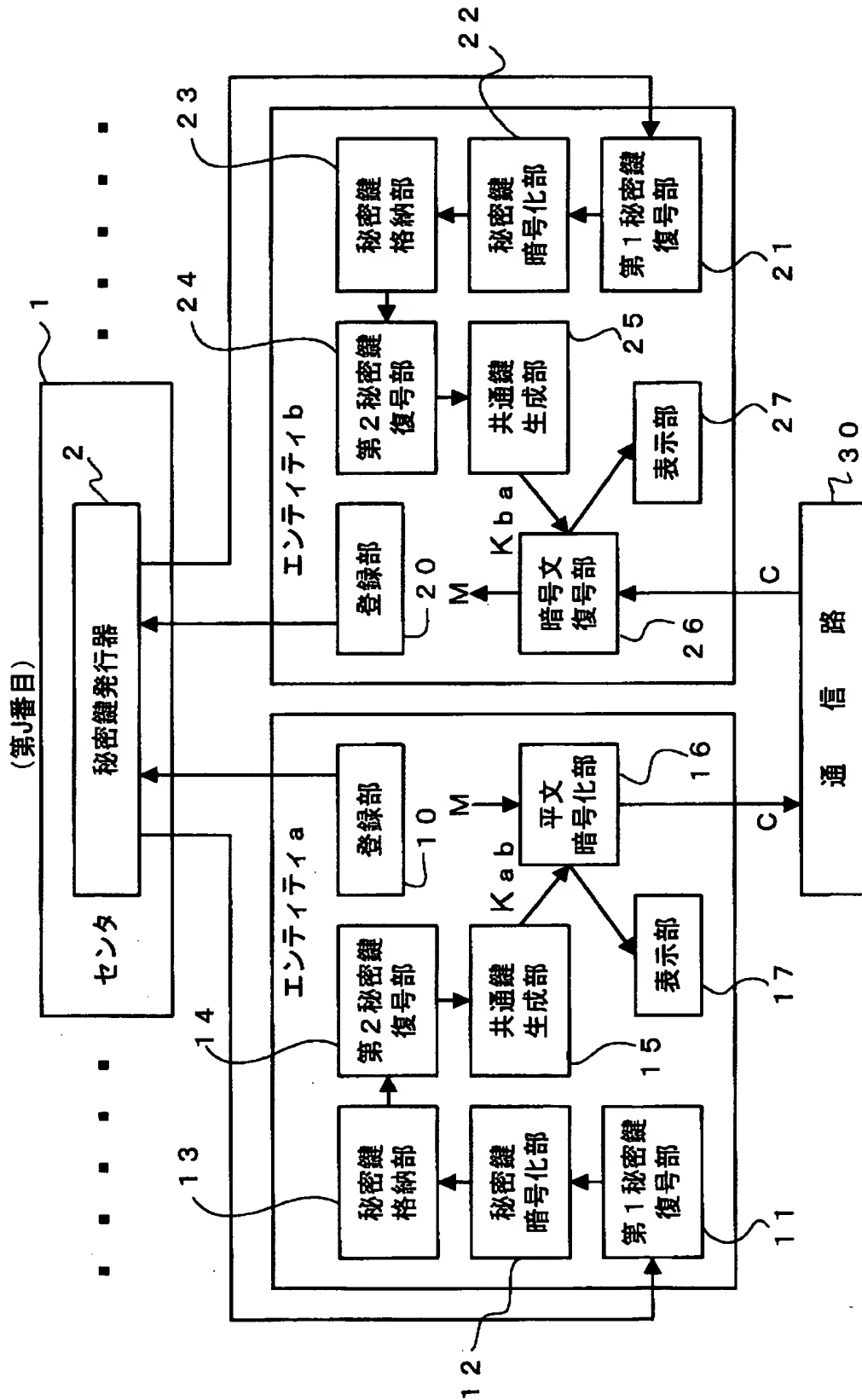
a, b, z エンティティ

【書類名】 図面

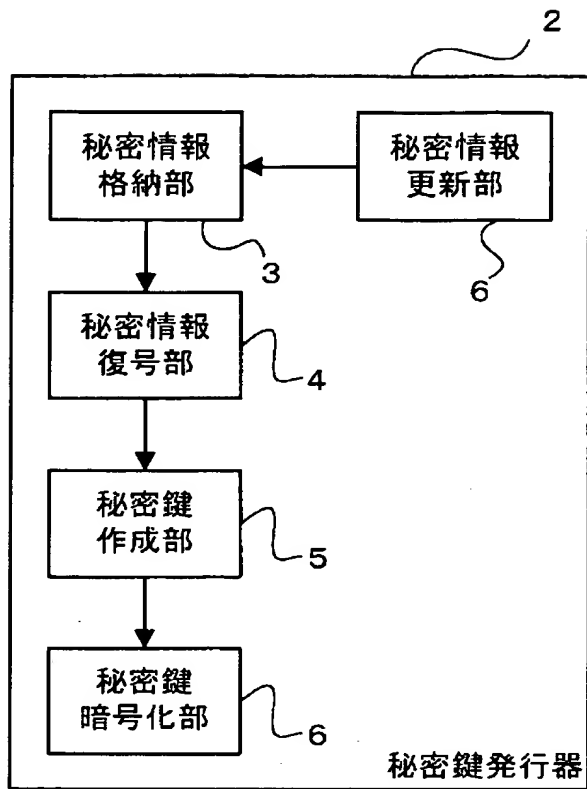
【図 1】



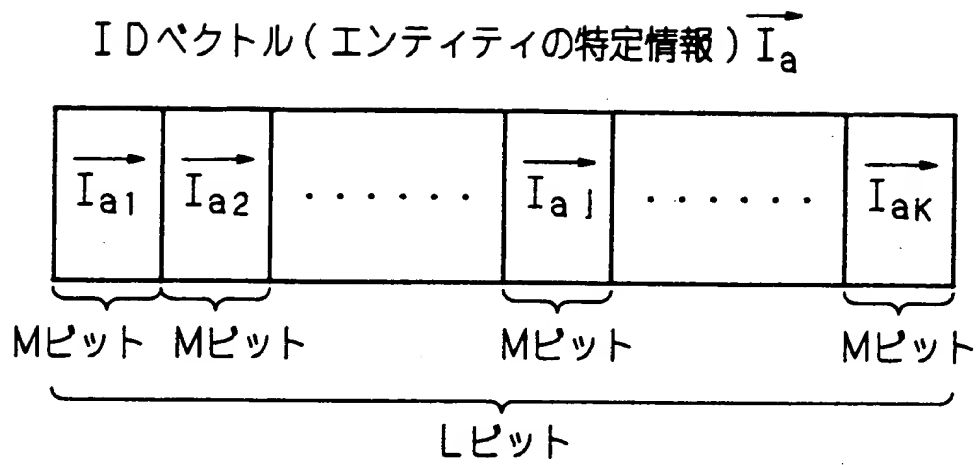
【図 2】



【図 3】

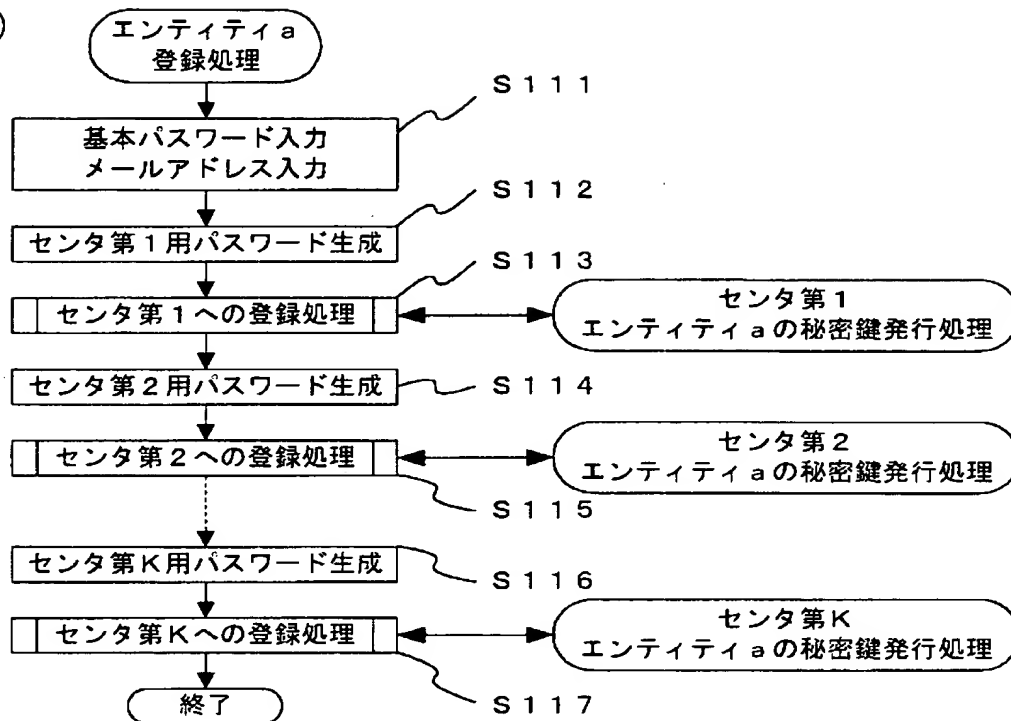


【図 4】

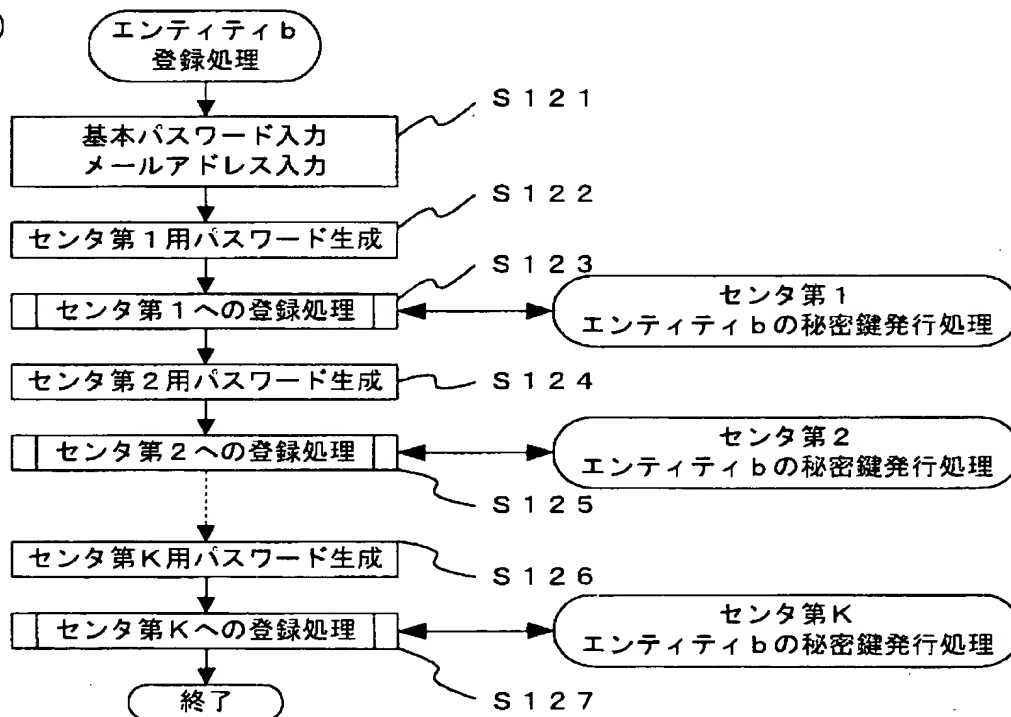


【図 5】

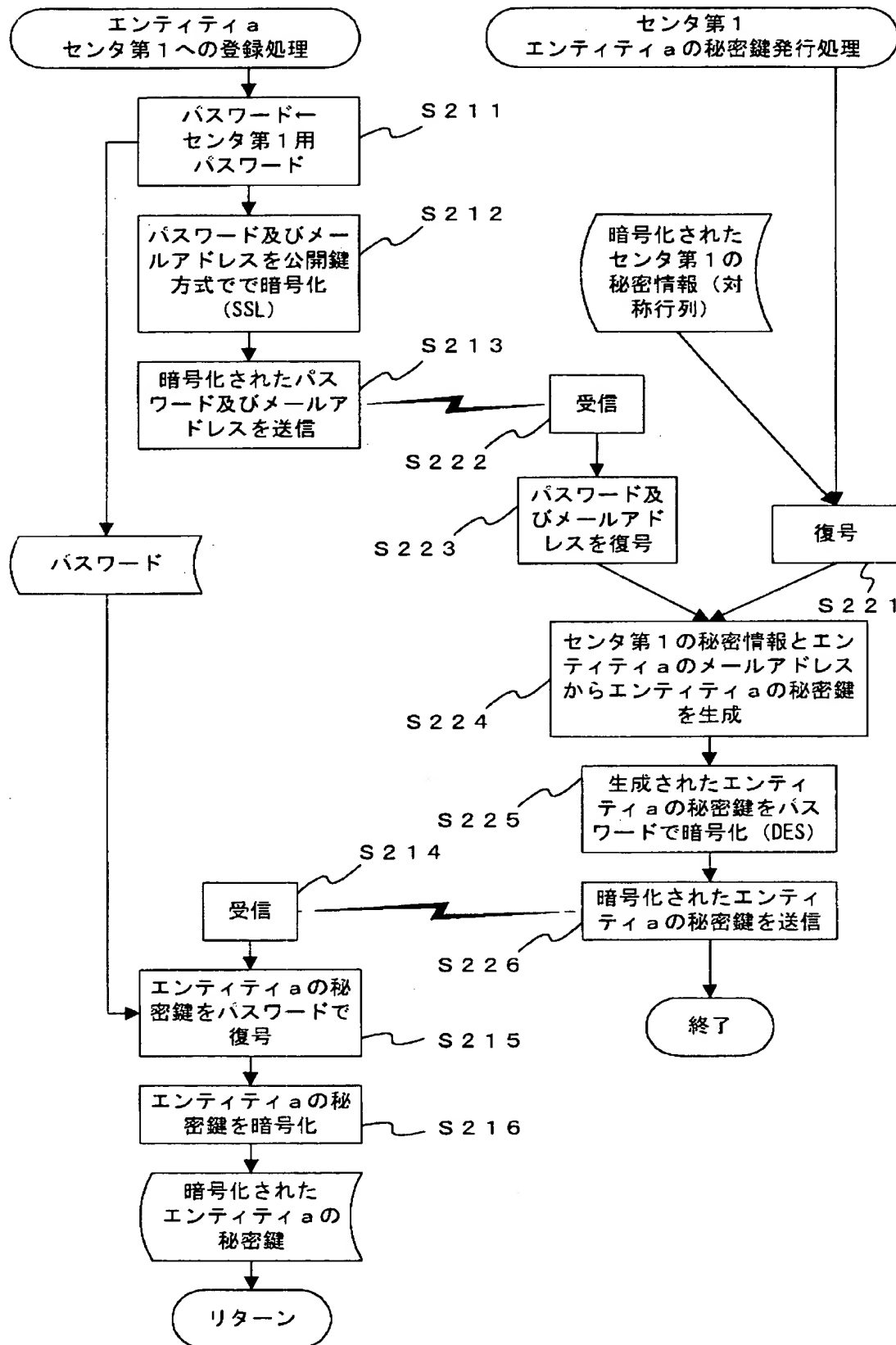
(I)



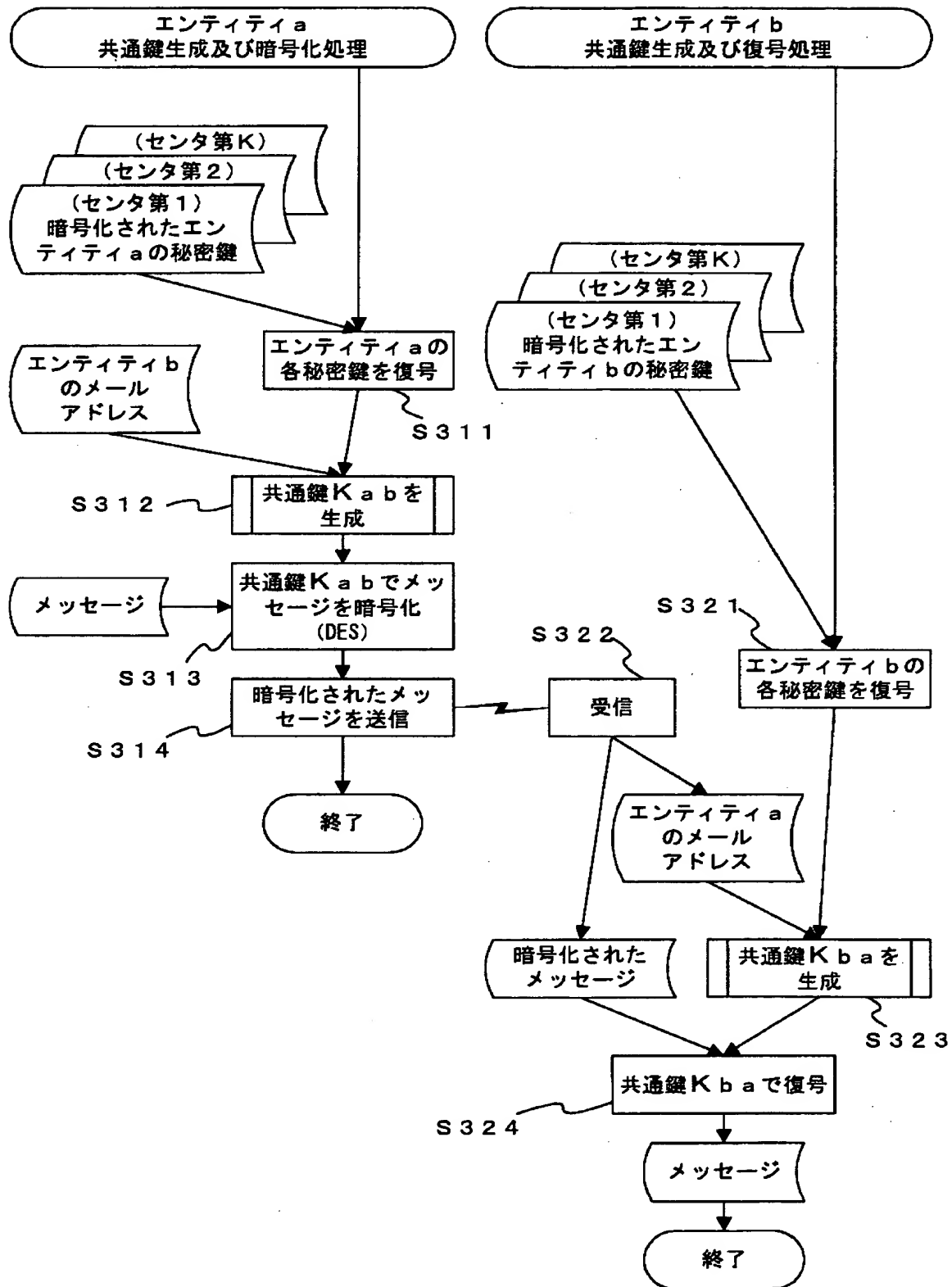
(II)



【図 6】



【図 7】



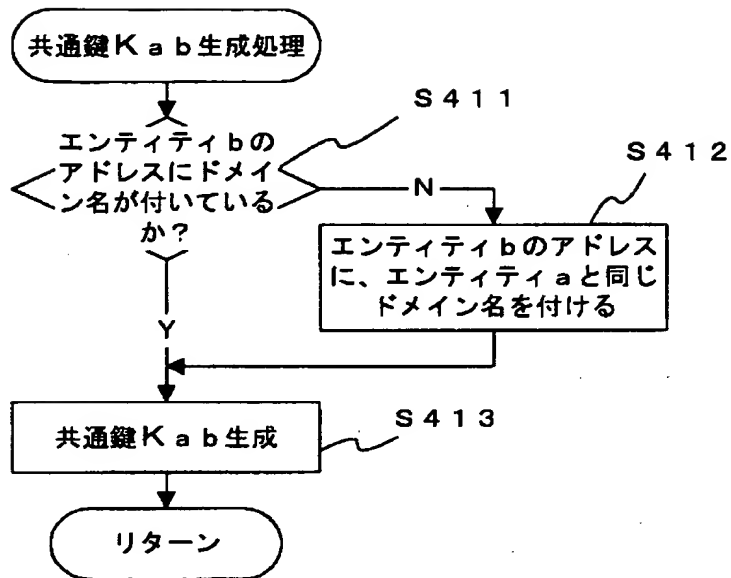
【図 8】

メールアドレスの例

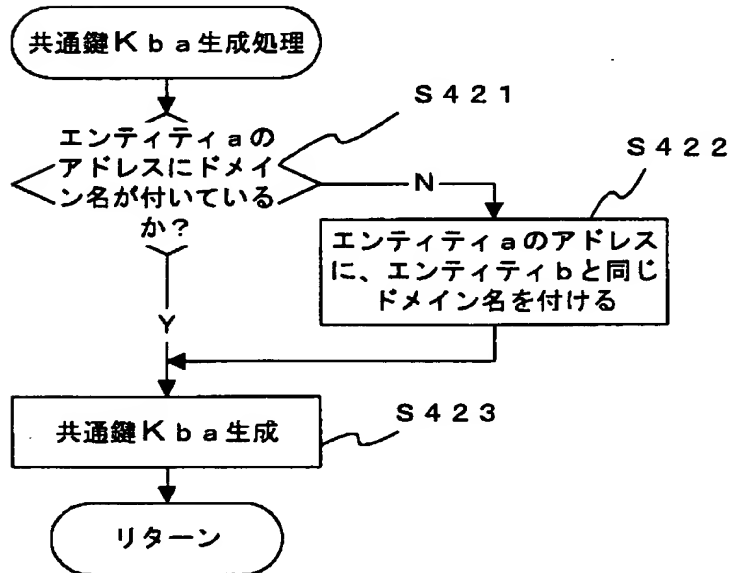
- | | |
|---------------------|---------------------------|
| (I) ドメイン名が付いている場合 | thomas@xyz.co.jp
ドメイン名 |
| (II) ドメイン名が付いていない場合 | thomas |

【図 9】

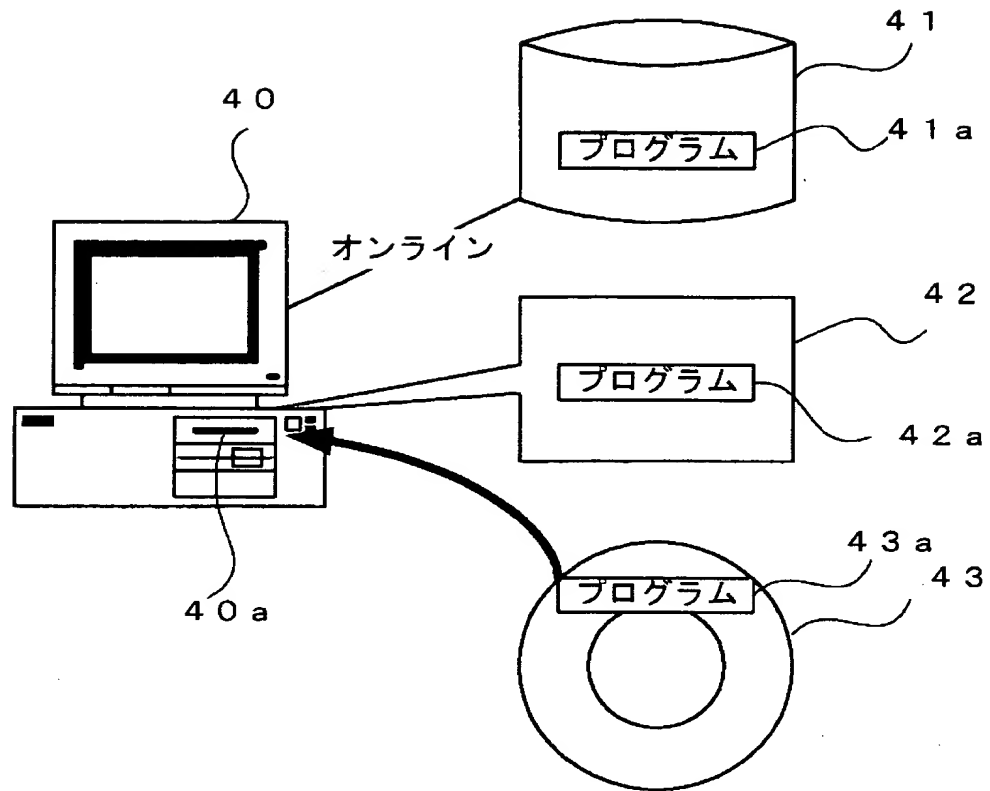
(I)



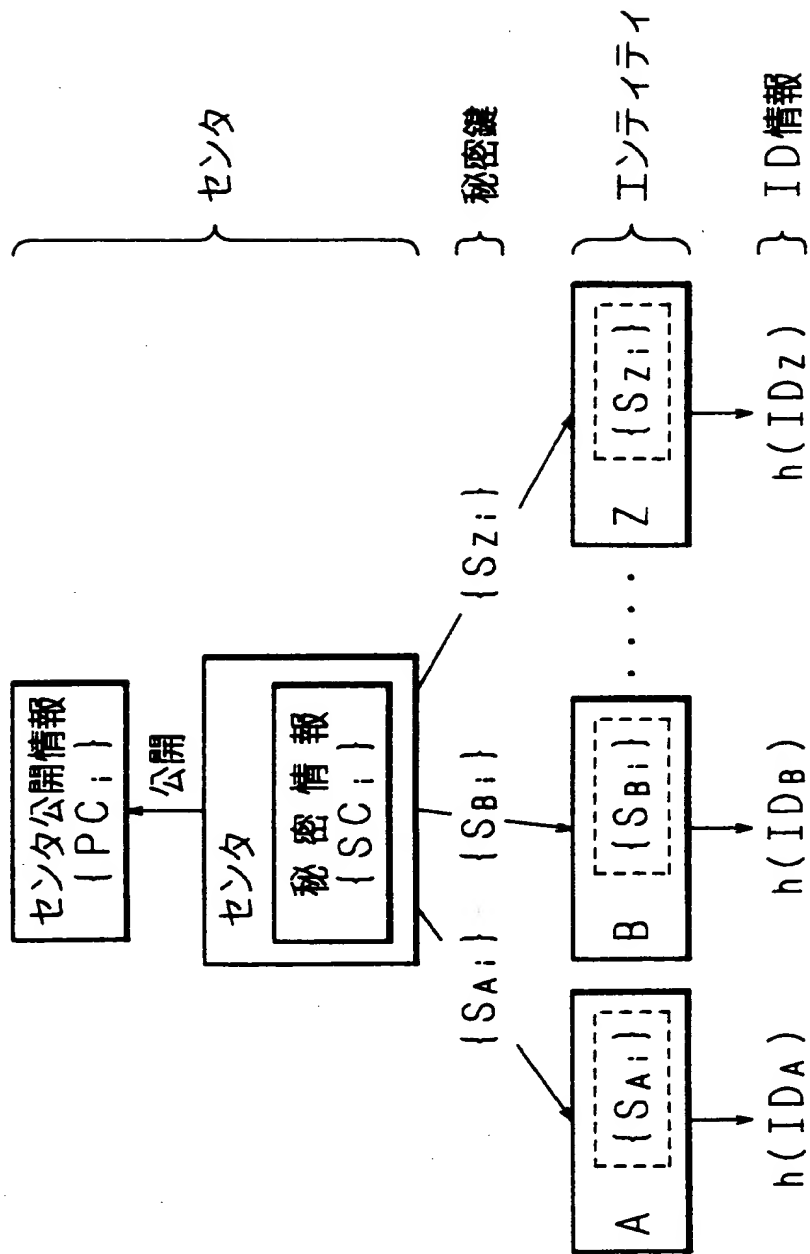
(II)



【図10】



【図 11】



【書類名】 要約書

【要約】

【課題】 複数の各センタから各エンティティへ秘密鍵を安全かつ容易に発行することができるようにする。

【解決手段】 各エンティティが、基本パスワードと一方向性変換関数に基づいて複数のパスワードを生成し、各センタへ送付するようにした。このパスワードは、各エンティティが、各センタから発行された各エンティティ固有の秘密鍵を安全に受け取るために使用される。各エンティティにおいて、管理しなければならないパスワードの数を少なくすることができる。

【選択図】 図 5

認定・付加情報

特許出願の番号	特願 2 0 0 0 - 0 1 6 3 6 3
受付番号	5 0 0 0 0 0 7 3 7 4 4
書類名	特許願
担当官	岡田 幸代 1 7 1 7
作成日	平成 1 2 年 3 月 2 3 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000006297
【住所又は居所】	京都府京都市南区吉祥院南落合町 3 番地
【氏名又は名称】	村田機械株式会社

【特許出願人】

【識別番号】	597008636
【住所又は居所】	大阪府箕面市栗生外院 4 丁目 1 5 番 3 号
【氏名又は名称】	笠原 正雄

【復代理人】

【識別番号】	100114557
【住所又は居所】	大阪府大阪市中央区釣鐘町二丁目 4 番 3 号 河野 特許事務所
【氏名又は名称】	河野 英仁

【代理人】

【識別番号】	100078868
【住所又は居所】	大阪府大阪市中央区釣鐘町二丁目 4 番 3 号 河野 特許事務所
【氏名又は名称】	河野 登夫

出 願 人 履 歴 情 報

識別番号 [000006297]

1. 変更年月日	1990年 8月 7日
[変更理由]	新規登録
住 所	京都府京都市南区吉祥院南落合町3番地
氏 名	村田機械株式会社

出 願 人 履 歴 情 報

識別番号 [597008636]

1. 変更年月日	1997年 1月21日
[変更理由]	新規登録
住 所	大阪府箕面市栗生外院4丁目15番3号
氏 名	笠原 正雄